Cyber Space, Sovereignty and the Intricacies of International Law-Making

Florian Kriener 2021-04-16T08:00:27

On March 5th, 2021, Germany published its position paper "On the application of International Law in Cyberspace". The inter-ministerial document stipulates Germany's views on the rules regulating state activity in cyberspace in a concise, well-founded and comprehensive manner. For this, Germany has been applauded by leading scholars in the field.

This blogpost highlights and critically assesses two issues raised in the position paper. First, it delves into the multi-layered protection of sovereignty advanced by Germany. Then, the blogpost unravels Germany's methodological approach to the rule of territorial sovereignty. Based on these two assessments, the position paper is situated within the intricate process of shaping the rules protecting sovereignty in cyber space.

Current developments in the international law of cyberspace

The rules of international law applicable in cyberspace have been under discussion by states throughout the last years. The majority of negotiations and deliberations take place within the United Nations Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (GGE) and the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG). The GGE published widely acknowledged and referenced reports in 2013 and 2015. However, the recent sessions of the GGE have not yielded results due to controversies among the member states. Similarly, the OEWG's final report, published only shortly after the German position paper, is rather thin on international law (paras. 34-40). It briefly restates that international law applies to cyberspace and only calls upon states to deepen their understanding on the matter. It does not contribute to the current contentious questions in the field.

Against the backdrop of this temporary impasse at the multilateral level, states have moved to publish their views on the applicable law in cyberspace unilaterally. Since 2019 alone, Australia, Estonia, Finland France, Israel, Iran, the Netherlands, New Zealand, the United Kingdom, the United States, and NATO have either published written positions or addressed the issue in public speeches through leading government officials. The German position paper adds to the effort of using unilateral declarations as well as multilateral fora to clarify international law's application in cyberspace.

In Germany's view, existing international law applies to state activity in cyberspace. The title already reflects this firm position reading "On the Applicat*ion*" rather than "On the Applic*ability*", rejecting arguments of a "legal vacuum" in cyberspace.

Accordingly, the German position paper comprehensively outlines the content and modalities through which international law applies to cyber operations, covering general International Law, International Humanitarian Law and the Law of State Responsibility. Michael Schmitt has already provided a thorough analysis of these positions within the ongoing discussions (here and here). Therefore, this analysis will take a closer look at two specific issues.

The multi-layered protection of sovereignty

Section II (p. 2 ff.) of the position paper discusses the three rules protecting state sovereignty. The gravest violation of a state's sovereignty, a violation of the prohibition of the use of force, uncontroversially applies to cyber operations. Germany takes the view that cyber operations constitute a use of force if their "scale and effect" are comparable to the use of kinetic weapons. This is in line with the ICJ's reasoning in the Nicaragua judgment (para. 195), where it held that an armed attack could be distinguished from a mere frontier incident based on its scale and effects. Accordingly, the physical impact of a measure is key to determine whether it surpasses the threshold of a prohibited use of force. Australia, Finland, the Netherlands, and New Zealand have likewise adopted this standard.

The position paper applies the same standard to the second layer of the protection of sovereignty, the prohibition of wrongful intervention. Accordingly, a violation of the prohibition of wrongful intervention can be assumed if the impact of a cyber-operation is "comparable in scale and effect to coercion in non-cyber contexts". This in turn implies "that a State's internal processes regarding aspects pertaining to its domaine réservé are significantly influenced or thwarted and that its will is manifestly bent by the foreign State's conduct." This clear position is notable. With regard to the prohibition of the use of force, the scale and effect doctrine draws on the reasoning of the Nicaragua judgment and is largely accepted as the pertinent standard for determining a use of force. In contrast, no international judgment or authoritative resolution establishes a standard for the determination of coercion. The Nicaragua judgment merely affirms that the prohibition of wrongful intervention protects the right of a state to decide freely on matters pertaining to its domaine réservé (para. 205). Consequently, several contradictory theories (here and here) on measuring coercion exist and states rarely explain what standard they apply when determining whether a state is thwarted from deciding freely on a manner in its domaine réservé. Placing the scale and effect of a measure of interference – and thus its impact on the exercise of a state's free will – at the center of an assessment of coercion, is only one of the possible options. Other approaches focus on the intent of the influencing state, the means of influence employed, and/or the reaction of the influenced state (find an excellent overview here). Therefore, Germany's clear position on this question is significant both in the cyber context and beyond.

Germany demonstrates the pertinence of the "scale and effect" standard with regard to the controversial question of foreign electoral interference (p.5). The conduct of elections is without doubt an aspect pertaining to a states domaine réservé. However, influences in electoral processes have been common, manifold and to some extent accepted throughout history. Dividing illegal interventions from legal influences is, hence, a difficult task. According to Germany, for an interference to

pass the threshold of coercion, it must "significantly imped[e] the orderly conduct of an election". The three envisioned modalities are, first, the impairment of electoral infrastructure that significantly modifies electoral results, second, disinformation campaigns via the internet that incite violent political upheaval, riots or civil strife, and, third, cyber activities that substantively disturb the political system by i.e. disenfranchising significant groups of citizens from voting. The impact of these three measures is sufficiently grave that the electoral process does not result in the proper expression of the electorate's will. Therefore, a state cannot exercise its sovereign right to freely determine its own government. Its sovereignty is thwarted. Requiring a significant impediment of the conduct of an election is thus a pertinent application of the coercion threshold to electoral interference.

The rule of territorial sovereignty

Additionally, Germany envisions a third rule protecting sovereignty in cyberspace below the prohibition of wrongful intervention. According to the rule of territorial sovereignty all states have the exclusive right to fully exercise their authority on their territory. Germany considers cyber operations to violate this rule if they produce "physical effects and harm" or cause "functional impairments" to cyber infrastructure on the territory of a state, particularly if this infrastructure is considered critical.

Viewing sovereignty not only as a principle but also as a rule has gained traction among states in recent years. Its conception is a reaction to the realities of state interaction in cyber space, where most state cyber operations do not breach the threshold of a use of force or coercion. Nonetheless, states wish to outlaw operations that disrupt or impair their cyber infrastructure, even if the exercise of their free will is not significantly impaired. To this end, they have been advocating for the recognition of the rule of territorial sovereignty. While this seems reasonable at first glance, a rule of territorial sovereignty can dilute the prohibition of wrongful intervention if the scope of the rule is not sufficiently restricted. This could be a critical development, as an extensive understanding of coercion could prohibit other low intensity interferences, such as democracy promotion, which Germany frequently engages in. The delimitation between the rule of territorial sovereignty and the prohibition of wrongful intervention thus merits a closer look.

To establish the rule of territorial sovereignty, the German position paper refers to the sovereign right of every state to freely choose its political, social, economic, and cultural system, which includes the field of information and communication technologies. This assertion is without doubt correct. However, it is precisely the definition employed by the Nicaragua judgment (para. 205) and the Friendly Relations Declaration for the domaine réservé of states. Germany only restricts the rule of territorial sovereignty with regard to the intensity of physical effects and functional impairments, excluding negligible impacts from violating the rule. This restriction, being something of a coercion "light" standard, barely restricts the scope of the rule of territorial sovereignty vis-à-vis the prohibition of wrongful intervention. *Ratione materiae* both rules overlap, operating with a different standard of coercion. This would entail a dilution of the prohibition of wrongful intervention.

The delimitation between the rule of territorial sovereignty and the prohibition of territorial sovereignty should focus on the *ratione materiae* application of the rule of territorial sovereignty. It is conceivable that some limited aspects of state authority should remain free of any outside influence. However, this area should be significantly smaller than the domaine réservé. If both rules' scope of application are equal, as the German argument suggests, the validity of the coercion criteria is drawn into doubt. This would however contradict the ICJ's jurisprudence whereby coercion is the "very essence of, prohibited intervention" and could furthermore constitute an undesirable development, as outlined above.

The intricacies of international law-making

Germany's stance on the rule of territorial sovereignty further raises methodological questions. Before the cyber debate kicked off, any attempt to establish a rule protecting sovereignty beneath the threshold of coercion was futile. Paradigmatically, a UN General Assembly resolution from 1981 titled "Declaration on the Inadmissibility of Intervention *and Interference* in the Internal Affairs of States" was thoroughly rejected by Western states and has not been able to shape the development of the (customary) international law protecting sovereignty. Accordingly, the rule of territorial sovereignty does not build on a prior established rule of customary international law and would require a settled state practice and corollary *opinio juris* to come into existence. To date, such settled practice does not exist.

Nonetheless, Germany is very firm on its stance that the rule of territorial sovereignty exists and forms part of positive international law. Germany avoids dealing with the problem of scarce state practice by framing its analysis of the rule of territorial sovereignty as an interpretation of the United Nations Charter. The section heading for the rule reads "Obligations of States derived from the United Nations Charter" (p. 2) and the applicable methods of interpretation cited later in the paper are arts. 31 et seq of the Vienna Convention on the Law of Treaties. However, art. 2 para. 1 of the United Nations Charter only contains the principle of sovereign equality. Likewise, the cases cited in favor of the rule of territorial sovereignty by Germany exclusively deal with the protection of sovereignty in customary international law (Island of Palmas Arbitration, Corfu Channel Case). Framing the matter as an interpretation of the United Nations Charter is thus a smoke screen to distract from the missing state practice in the field.

However, in order to achieve its goal of establishing the rule of territorial sovereignty, Germany has to take an assertive stance on this question. Only if Germany is firm on this question will its statement be considered *opinio juris* and potentially verbal state practice. Accordingly, Germany can only contribute to the emergence of the rule, if it prematurely argues that this rule already positively exists. This intricacy of international law-making thus explains the methodological backward bend taken with regard to the rule of territorial sovereignty.

What next?

The foregoing analysis demonstrates the timeliness and importance of the German position paper. As international law in cyber space is under development at the moment, it is important for states to take a firm stance on the open questions, in order to advance the clarification (and creation) of international law. With regard to the protection of sovereignty in cyber space, it would be preferable if the rule of territorial sovereignty were delineated *ratione materiae* from to the prohibition of wrongful intervention. The position paper suggests an extensive overlap between the two rules, which would contradict standing customary international law and constitute a critical dilution of the coercion standard.

Ideally, the refinement of Germany's position can take place within the GGE. Consultations and deliberations on the final report are scheduled for May 2021. The Biden Administration's renewed push on this matter could provide a decisive impulse, paving the way for the 25-member body to adopt a report by consensus. However, if consensus cannot be reached, it will be up to individual states to publish their views in the form Germany just has, to further develop and clarify the international law applicable in cyberspace.
